RE: New contact information for RC6™

During Round 2 of the AES, the following contact information should be used for the submitters of RC6™, instead of the contacts listed on the attached original cover sheet:

Primary contact

Burt Kaliski
Chief Scientist and Director
RSA Laboratories
20 Crosby Drive
Bedford, MA 01730
USA
TEL: +1 781 687 7057
FAX: +1 781 687 7213
burt@rsa.com

Backup contact

Magnus Nyström
Manager, RSA Laboratories Europe
Box 107 04 / Arenavägen 29
121 29 Stockholm
Sweden
TEL: +46 8 725 97 95
FAX: +46 8 649 49 70
mnystrom@rsasecurity.com

RSA Data Security.
A Security Dynamics Company

100 Marine Parkway
Suite 500
Redwood City
California, 94065-1031
415/595-8782 voice
415/595-1873 fax
http://www.rsa.com

May 28, 1998

DIRECTOR, INFORMATION TECHNOLOGY LABORATORY
Attn: Advanced Encryption Standard Nominations
Technology Building
Room A231
National Institute of Standards and Technology
Gaithersburg, MD 20899

Dear Sir,

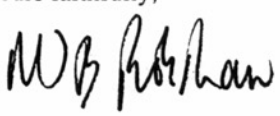
Please find enclosed details of a candidate block cipher for the new Advanced Encryption Standard (AES).

Name of algorithm:	RC6 ™
Principal submitter:	RSA Laboratories Represented by Matthew J.B. Robshaw Principal Research Scientist RSA Laboratories 2955 Campus Drive Suite 400 San Mateo, CA 94403 Ph: (650) 295-7600 Fax: (650) 295-7713 E-mail: matt@rsa.com
Auxiliary submitter:	Ronald L. Rivest
Algorithm inventors:	Ronald L. Rivest, Matthew J.B. Robshaw, Ray Sidney, Yiqun Lisa Yin
Algorithm owner:	RSA Data Security, Inc.
Backup point of contact:	Yiqun Lisa Yin Senior Research Scientist RSA Laboratories 2955 Campus Drive Suite 400 San Mateo, CA 94403 Ph: (650) 295-7600 Fax: (650) 295-7713 E-mail: yiqun@rsa.com

I have been asked to mention that RC6 is a trademark of RSA Data Security used in connection with its licensing of software product implementations. It is our understanding and expectation that if the submission from RSA Data Security for the AES is selected, the government will ascribe its own name identifying the underlying technology. At such point, RSA Data Security may continue to license and distribute its software and other products implementing the AES algorithm under its RC6 mark.

Finally, we would like to thank yourself and NIST for the useful and prompt feedback on our preliminary submission of April 15, 1998 which has helped us in preparing our final submission.

Yours faithfully,



Matthew J.B. Robshaw

Principal Research Scientist
RSA Laboratories

Enc:	The RC6 ™ Block Cipher	(document)
	Statements Regarding RC6 ™	(document)
	Statement of submitter	(document)
	Statement of patent holder	(document)
	Statement of implementation owner	(document)
	Statement of copyright	(document)
	9 Diskettes	